LAPORAN

PENELITIAN DASAR PENGEMBANGAN PROGRAM STUDI

PENGKODEAN HURUF HIJAIYAH UNTUK DETEKSI DAN KOREKSI KESALAHAN PENULISAN AYAT AL-QUR'AN MENGGUNAKAN KODE LINEAR

OLEH :

1. **Muhamad Zaki Riyanto, M.Sc. (Ketua)**
2. **Yenni Kartika (Asisten Peneliti)**
3. **Nenti Ekta Monita Larasati (Asisten Peneliti)**

FAKULTAS SAINS DAN TEKNOLOGI

UIN SUNAN KALIJAGA

YOGYAKARTA

2019

KATA PENGANTAR

Laporan Penelitian BOPTN 2019 dengan judul "Pengkodean Huruf Hijaiyah Untuk Deteki dan Koreksi Kesalahan Penulisan Ayat Al-Qur'an Menggunakan Kode Linear" merupakan salah satu wujud integrasi dan interkoneksi antara ilmu matematika dan duia Islam, yaitu pemanfaatan ilmu aljabar yang dapat dimanfaatkan untuk deteksi dan koreksi kesalahan penulisan dalam huruf hijaiyah.

Laporan penelitian ini menjabarkan dan penerapan dari konep-konsep dalam ilmu aljabar, khususnya teori pengkodean yang digunakan untuk deteksi dan koreksi penulisan dalam huruf hijaiyah. Konsep-konsep tersebut adalah: (1) Dasar struktur aljabar yang meliputi konsep dasar grup, ring, lapangan, ruang vektor, subruang, basis dan dimensi. (2) Dasar teori pengkodean yang meliputi pengertian kode linear, jarak Hamming, matriks generator dan matriks cek paritas. (3) Kode Hamming yang memiliki kemampuan koreksi sebanyak satu kesalahan, serta cara konstruksi dan metode koreksinya melalui matriks cek paritas. (4) Korespondensi antara huruf hijaiyah melalui ekspansi biner sepanjang 5 bit dari bilangan sesuai dengan urutannya dalam huruf hijaiyah.

Peneliti menyadari bahwa masih banyak kekurangan dalam laporan penelitian ini. Oleh karena itu, peneliti sangat mengharapkan kritik maupun saran agar laporan penelitian ini dapat lebih baik lagi. Kritik dan saran tersebut dapat disampaikan melalui email peneliti di zaki.riyanto@uin-suka.ac.id

Berkat dukungan dari berbagai pihak, khususnya dari LPPM UIN Sunan Kalijaga Yogyakarta, telah sangat membatu pelaksanaan penelitian ini. Untuk itu, peneliti mengucapkan banyak terima kasih yang sebesar-besarnya kepada semua pihak yang telah turut serta membantu pelaksanaan penelitian ini.

Yogyakarta, 15 November 2019

Peneliti

ABSTRAK

Huruf hijaiyah memainkan peran yang sangat penting dalam dunia Islam, salah satu alasannya karena Al-Qur'an ditulis dalam huruf Arab yang menggunakan huruf hijaiyah. Perkembangan teknologi memudahkan setiap orang untuk menulis dan menyebarkan ayat-ayat Al-Qur'an dalam berbagai media elektronik. Akan tetapi, terkadang dijumpai kesalahan penulisan yang dapat merubah arti dan makna dari suatu ayat. Di dalam ilmu aljabar, dikenal teori pengkodean yang mempelajari bagaimana suatu pesan itu dikodekan, sehingga memiliki kemampuan deteksi dan koreksi kesalahan yang terjadi pada saat pengiriman pesan. Saat ini teori pengkodean telah digunakan secara luas untuk mengangani kesalahan dalam pengiriman maupun penyimpanan data dalam media elektronik, seperti hardisk, flashdisk, serta jaringan internet dan seluler. Salah satu jenis kode yang sering digunakan adalah kode linear yang dikonstruksi melalui sebuah subruang dari suatu ruang vektor atas lapangan hingga.

Kode linear dapat diterapkan untuk deteksi dan koreksi kesalahan penulisan pesan dalam huruf hijaiyah. Oleh karena itu, perlu dikaji cara mengkonstruksi korespondensi huruf hijaiyah agar dapat dikodekan menggunakan kode linear, juga perlu diketahui jenis kesalahan seperti apa yang dapat dideteksi dan dikoreksi menggunakan kode linear, dan terakhir adalah bagaimana cara mendeteksi dan mengkoreksi kesalahan penulisan dalam huruf hijaiyah menggunakan kode linear.

Dalam penelitian ini, lapangan hingga yang digunakan adalah lapangan biner. Oleh karena itu, setiap huruf hijaiyah harus dikorespondensikan dengan ekspansi biner sesuai dengan urutan hurufnya dengan panjang 5 bit. Kode linear yang digunakan adalah kode Hamming berorder 3 atas lapangan biner, dengan matriks generator berupa matriks biner berukuran 4x7, dan matriks cek paritas berupa sebuah matriks biner berukuran 3x7. Matriks generator digunakan untuk mengkodekan, sedangkan matriks cek paritas digunakan untuk mendeteksi dan mengkoreksi kesalahan. Jenis kesalahan penulisan yang dapat dideteksi dan dikoreksi adalah dalam setiap blok pesan yang terdiri dari 4 huruf hijaiyah hanya boleh ada 1 huruf yang berubah menjadi huruf hijaiyah yang lainnya. Konsekuensi dari adanya pengkodean ini adalah bertambahnya panjang setiap blok pesan, dari yang semula memiliki panjang 20 bit, setelah dikodekan menjadi 35 bit, atau terjadi penambahan cek bit sebesar 15 bit.

Kata kunci: kode linear, huruf hijaiyah, lapangan hingga, teori pengkodean

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1. LATAR BELAKANG

Al-Qur'an merupakan pegangan hidup dari setiap muslim untuk mengarungi kehidupan sampai di hari kiamat. Al-Qur'an diturunkan oleh Allah s.w.t. melalui malaikat Jibril kepada Nabi Muhammad s.a.w. sebagai nabi untuk umat manusia. Di dalamnya terdapat berbagai perintah, larangan, kisah dan hal-hal lainnya yang menakjubkan. Al-Qur'an senantiasa dijaga keasliannya oleh Allah sebagai salah satu bukti kebenaran dan kemukjizatannya, sebagaimana telah difirmankan Allah dalam Surat Al-Hijr ayat 9:

إِنَّا نَحْنُ نَزَّلْنَا الذِّكْرَ وَإِنَّا لَهُ لَحَافِظُونَ.

yang artinya: "Sesungguhnya Kami yang menurunkan al-Qur`an dan Kami sendiri yang akan menjaganya." (Qs. Al-Hijr : 9).

Salah satu cara Allah s.w.t menjaga keaslian Al-Qur'an adalah dengan membuatnya mudah dihafalkan bahkan oleh orang yang bahasa ibunya bukan bahasa arab. Hingga kini telah ada banyak orang yang mampu menghafalkan Al-Qur'an. Sebagaimana difirmankan oleh Allah dalam Surat Al-Qomar ayat 17:

وَلَقَدْ يَسَّرْنَا الْقُرْآنَ لِلذِّكْرِ فَهَلْ مِن مُّدَّكِرٍ ﴿٢٣﴾

yang artinya: "Dan sesungguhnya Kami mudahkan al-Quran untuk pelajaran, maka adalah orang yang mau mengambil pelajaran." (Qs. Al-Qomar: 17).

Perkembangan teknologi dapat memudahkan penulisan Al-Qur'an dalam berbagai media cetak dan elektronik. Akan tetapi, tidak ada hal yang sempurna di dunia ini, manusia dapat melakukan kesalahan, baik itu disengaja maupun tidak disengaja. Tak terkecuali dalam penulisan ayat Al-Qur'an. Tak jarang dijumpai kasus kesalahan penulisan ayat Al-Qur'an, seperti pada kasus kesalahan penulisan oleh seseorang yang ditayangkan di sebuah televisi swasta nasional. Kasus lain tentang kesalahan penulisan ayat Al-Qur'an juga ditemui pada beberapa buku Pendidikan Agama Islam (Republika, 29 Oktober 2017).

Salah satu cara untuk menyelesaikan tersebut adalah melakukan pengkodean huruf hijaiyah yang digunakan dalam penulisan ayat menggunakan teori pengkodean. Teori pengkodean bermula dari penelitian Shannon (1948). Oleh Shannon dijelaskan konsep awal tentang teori pengkodean untuk pendeteksian adanya kesalahan dan kemungkinan dalam melakukan koreksinya. Hingga saat ini, teori pengkodean telah berkembang pesat, sehingga memunculkan berbagai jenis kode, salah satunya adalah kode linear (Jurgen Bierbrauer, 2016).

Teknik pengkodean huruf hijaiyah telah dilakukan oleh Yahya Alqahtani dkk (2013), dilanjutkan oleh Prakash Kuppuswamy dan Yahya Alqahtani (2014) untuk enkripsi pesan rahasia dalam huruh hijaiyah. Perkembangan pengkodean huruf hijaiyah terus dilakukan oleh Ameer Kadhim Hadi (2017) untuk pengamanan pesan rahasia. Akan tetapi, dari penelitian-penelitian tersebut belum menyinggung tentang pengkodean untuk kepentingan deteksi dan koreksi kesalahan penulisan teks menggunakan huruf hijaiyah.

Dalam penelitian ini, adanya kesalahan dalam penulisan dalam huruf hijaiyah akan dideteksi dan dikoreksi menggunakan kode linear, proses perhitungannya dilakukan pada suatu subruang dari ruang vektor yang dikonstruksi melalui sebuah matriks tertentu. Oleh karena itu, perlu dikonstruksi suatu korespondensi antara huruf hijaiyah dengan vektor.

1.2. RUMUSAN MASALAH

Berdasarkan latar belakang masalah yang ditemukan pada kesalahan penulisan ayat Al-Qur’an dan kode linear yang digunakan untuk deteksi dan koreksi kesalahan, maka dalam penelitian dapat dibentuk rumusan masalah yaitu:

a. Bagaimana cara mengkonstruksi korespondensi huruf hijaiyah dan pengkodeannya menggunakan kode linear.
b. Bagaimana jenis kesalahan penulisan dalam huruf hijaiyah yang dapat dikoreksi menggunakan kode linear
c. Bagaimana cara mendeteksi dan mengkoreksi adanya kesalahan penulisan dalam huruf hijaiyah yang telah dikodekan menggunakan kode linear.

1.3. TUJUAN PENELITIAN

Berdasarkan rumusan masalah yang telah ditetapkan di atas, penelitian ini bertujuan untuk:

a. Mengetahui korespondensi huruf hijaiyah kode linear untuk pengkodean huruf hijaiyah.
b. Mengetahui jenis kesalahan penulisan dalam huruf hijaiyah yang dapat dikoreksi menggunakan kode linear.
c. Menganalisis cara mendeteksi dan mengkoreksi adanya kesalahan penulisan dalam huruf hijaiyah yang telah dikodekan menggunakan kode linear.

1.4. MANFAAT PENELITIAN

Penelitian ini memiliki manfaat mengatasi kesalahan jenis tertentu pada penulisan dalam huruf hijaiyah, contohnya adalah dalam penulisan ayat Al-Qur’an secara modern dengan bantuan komputasi digital berdasarkan teori matematika. Hal tersebut dilakukan untuk mencegah terjadinya kesalahan penulisan ayat Al-Qur’an dengan lebih cepat sebelum beredar luas di masyarakat. Selain itu, penelitian ini juga untuk melaksanakan konsep integrasi-interkoneksi antara sains dan agama, khususnya ilmu aljabar yang ternyata memiliki manfaat yang luar biasa bagi kehidupan manusia.

BAB II

TINJUAN PUSTAKA DAN LANDASAN TEORI

2.1. TINJAUAN PUSTAKA

Kode linear merupakan salah satu kode yang banyak digunakan dalam teknik pengkodean data yang disimpan maupun dikirimkan melalui media dan jalur komunikasi elektoronik, seperti CD, DVD, jaringan internet dan jaringan seluler. Teknik pengkodean sangat penting dilakukan, hal tersebut dikarenakan reliabilitas perangkat penyimpanan atau jalur komunikasi yang tidak dapat dijamin sempurna. Sebagai contoh dari tidak reliabilitas tersebut adalah dalam penyimpanan data dalam CD dan DVD yang sangat rentan tergores, sehingga dapat menyebatkan rusaknya data. Selain itu, pada jaringan seluler yang bersifat *wireless* melalui jalur udara sangat rentan terhadap gangguan cuaca maupun inferensi dengan perangkat yang lain.

Teknik pengkodean untuk deteksi dan koreksi kesalahan saat proses penyimpanan atau pengiriman data pertama kali dikembangkan oleh Shannon (1948) melalui artikelnya yang sangat terkenal yaitu 'A Mathematical Theory of Communication'. Perkembangan teori pengkodean semakin pesat pada era teknologi informasi saat ini. Setiap orang dapat berkomunikasi jarak jauh menggunakan internet dan jaringan seluler secara mudah dan murah. Setiap orang juga dapat menyimpan data-data dengan murah dan mudah, seperti dokumen dan foto dalam bentuk digital, menggunakan komputer dan telepon genggam. Beberapa kode yang digunakan secara luas saat ini adalah kode linear, kode siklik, kode Hamming, kode Reed-Muller, kode BCH, kode Reed-Solomon, kode Golay dan kode Goppa (Jurgen Bierbrauer, 2016). Kajian teknik pengkodean huruf hijaiyah mengacu pada hasil penelitian Yahya Alqahtani dkk (2013), Prakash Kuppuswamy dan Yahya Alqahtani (2014) dan Ameer Kadhim Hadi (2017).

2.2. LANDASAN TEORI

Secara umum, dalam teori pengkodean terdapat dua proses utama, yaitu *encoding* dan *decoding*. *Encoding* adalah proses merubah teks awal menjadi kode yang biasanya berupa angka-angka, sedangkan *decoding* adalah proses perubahan kode-kode menjadi teks semula. Pembahasan dalam teori pengkodean sangat membutuhkan dasar-

dasar aljabar yang meliputi struktur aljabar, yaitu teori grup, ring dan lapangan, serta aljabar linear yang meliputi konsep matriks, ruang vektor, subruang, basis dan dimensi.

2.2.1. GRUP

Definisi 2.2.1. (Thomas W. Judson, 2017) *Diberikan himpunan tak kosong G dan "$*$" adalah operasi biner pada G. Himpunan G disebut* ***grup*** *terhadap "$*$" jika memenuhi aksioma-aksioma berikut:*

(1) *Untuk setiap* $a,b,c \in G$ *berlaku* $a*(b*c)=(a*b)*c$

(2) *Terdapat* $e \in G$ *sehingga untuk setiap* $a \in G$ *berlaku* $a*e=e*a=a$. *Elemen e disebut dengan* ***elemen identitas***

(3) *Untuk setiap* $a \in G$ *terdapat* $b \in G$ *sehingga* $a*b=b*a=e$. *Elemen b disebut* ***invers*** *dari a, dituliskan dengan* $a^{-1}=b$.

Himpunan G yang dilengkapi dengan operasi "$*$" dinotasikan dengan $(G,*)$, *atau cukup dengan G saja apabila operasinya sudah diketahui, serta a*b dapat cukup ditulis dengan ab saja.*

Contoh 2.2.1. Berikut ini adalah contoh-contoh dari grup.

(1) Himpunan semua bilangan bulat $\mathbb{Z}$ merupakan grup terhadap operasi penjumlahan bilangan bulat biasa.

(2) Himpunan semua bilangan bulat modulo *m* yaitu $\mathbb{Z}_m=\{0,1,2,...,m-1\}$ merupakan grup terhadap operasi penjumlahan bilangan bulat modulo *m*, dengan *m* adalah bilangan bulat positif.

(3) Himpunan semua vektor baris dengan panjang *n* atas $\mathbb{Z}_m$, didefinisikan sebagai himpunan $V_n(\mathbb{Z}_m)=\{(x_1,x_2,...,x_n): x_1,x_2,...,x_n \in \mathbb{Z}_m\}$ adalah grup terhadap operasi penjumlahan vektor modulo *m*.

Definisi 2.2.2. (Thomas W. Judson, 2017) *Grup G disebut dengan* ***grup abelian*** *jika operasi binernya komutatif, yaitu untuk setiap* $a,b \in G$ *berlaku* $ab=ba$.

Contoh 2.2.2. Berikut ini adalah contoh-contoh dari grup abelian.

(1) Himpunan semua bilangan bulat $\mathbb{Z}$ merupakan grup abelian terhadap operasi penjumlahan bilangan bulat biasa.

(2) Himpunan semua bilangan bulat modulo *m* yaitu $\mathbb{Z}_m = \{0,1,2,...,m-1\}$ merupakan grup abelian terhadap operasi penjumlahan bilangan bulat modulo *m*, dengan *m* adalah bilangan bulat positif.

(3) Himpunan $V_n(\mathbb{Z}_m) = \{(x_1, x_2, ..., x_n) : x_1, x_2, ..., x_n \in \mathbb{Z}_m\}$ adalah grup abelian terhadap operasi penjumlahan vektor modulo *m*.

Definisi 2.2.3. (Thomas W. Judson, 2017) *Diberikan H adalah himpunan bagian tak kosong dari G, maka H disebut* ***subgrup*** *dari G jika H juga merupakan grup terhadap operasi yang sama pada grup G.*

Contoh 2.2.3. Berikut ini adalah contoh dari subgrup.

(1) Himpunan $H = \{0,2,4\}$ adalah subgrup dari grup $\mathbb{Z}_6$.

(2) Himpunan $C = \{(0,0),(0,2),(0,4)\}$ adalah subgrup dari grup $V_2(\mathbb{Z}_6)$.

Teorema 2.2.1. *Diberikan H adalah himpunan bagian tak kosong dari G, maka H adalah subgrup dari G jika dan hanya jika untuk setiap* $a,b \in H$ *memenuhi sifat* $ab^{-1} \in H$.

2.2.2. RING DAN LAPANGAN

Definisi 2.2.4. (Malik dkk, 1997) *Diberikan R adalah himpunan tak kosong, serta "+" dan "." adalah operasi-operasi pada R. Himpunan R disebut* ***ring*** *terhadap "+" dan "." jika memenuhi aksioma berikut:*

(1) *Himpunan R adalah grup abelian terhadap operasi "+". Elemen identitas dari R terhadap penjumlahan dinamakan dengan* ***elemen netral*** *dan dinotasikan* 0_R.

(2) *Untuk setiap* $a,b,c \in R$ *berlaku* $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(3) *Untuk setiap* $a,b,c \in R$ *berlaku* $a \cdot (b+c) = a \cdot b + a \cdot c$ *dan* $(a+b) \cdot c = a \cdot c + b \cdot c$.

Untuk selanjutnya, ring R disebut ***ring komutatif*** *apabila operasi perkalian bersifat komutatif, yaitu untuk setiap* $a,b \in R$ *berlaku* $a \cdot b = b \cdot a$. *Ring R disebut* ***ring dengan***

elemen satuan *jika terdapat* $1_R \in R$ *sehingga untuk setiap* $a \in R$ *berlaku* $a \cdot 1_R = 1_R \cdot a = a$. *Ring R disebut* ***lapangan*** *jika R adalah ring komutatif dengan elemen satuan dan untuk setiap elemen tak nol* $a \in R$ *terdapat* $a^{-1} \in R$ *sehingga* $a \cdot a^{-1} = a^{-1} \cdot a = 1_R$. *Ring R disebut* ***ring hingga*** *apabila memiliki anggota sebanyak berhingga.*

Contoh 2.2.4. Berikut ini adalah contoh-contoh ring.

1. Himpunan semua bilangan bulat $\mathbb{Z}$ adalah ring komutatif dengan elemen satuan terhadap operasi penjumlahan dan perkalian bilangan biasa. Ring $\mathbb{Z}$ bukanlah sebuah lapangan, sebab ada bilangan bulat 2 yang tidak memiliki invers terhadap operasi perkalian.
2. Himpunan semua bilangan real $\mathbb{R}$ adalah ring komutatif dengan elemen satuan terhadap operasi penjumlahan dan perkalian bilangan biasa, serta setiap bilangan real tak nol memiliki invers terhadap oprasi perkalain, sehingga $\mathbb{R}$ adalah suatu lapangan.
3. Diberikan p adalah bilangan prima, maka himpunan semua bilangan bulat modulo *p* yaitu $\mathbb{Z}_p = \{0,1,2,...,p-1\}$ adalah lapangan hingga terhadap operasi penjumlahan dan perkalian bilangan bulat modulo *p*. Dalam penelitian ini, lapangan hingga yang digunakan adalah lapangan $\mathbb{Z}_p$, lebih khusus adalah lapangan biner $\mathbb{Z}_2 = \{0,1\}$.

2.2.3. RUANG VEKTOR

Definisi 2.2.5. (Anton, 2014) *Diberikan* $(V, \oplus)$ *adalah grup abelian dan* $(F, +, \cdot)$ *adalah lapangan. Diberikan suatu operasi perkalian skalar* $\odot : F \times V \to V$. *Grup abelian V disebut* ***ruang vektor*** *atas lapangan F terhadap operasi perkalian skalar* $\odot$ *apabila memenuhi aksioma-aksioma berikut ini:*

(1) *Untuk setiap* $k \in F$ *dan* $u, v \in V$ *berlaku* $k \odot (u \oplus v) = (k \odot u) \oplus (k \odot v)$

(2) *Untuk setiap* $k, l \in F$ *dan* $u \in V$ *berlaku* $(k + l) \odot u = (k \odot u) \oplus (l \odot u)$

(3) *Untuk setiap* $k,l \in F$ *dan* $u \in V$ *berlaku* $(k \cdot l) \odot u = k \odot (l \odot u)$

(4) *Untuk setiap* $u \in V$ *berlaku* $1 \odot u = u$ *, dengan* 1 *adalah elemen satuan dari F.*

Selanjutnya, elemen dari ruang vektor V disebut dengan ***vektor****, dan elemen dari lapangan F disebut dengan* ***skalar****. Elemen identitas dari grup V disebut dengan* ***vektor nol****, dinotasikan dengan* $\bar{0}$*. Untuk mempersingkat penulisan, ruang vektor* $(V, \oplus)$ *cukup dituliskan dengan V, operasi penjumlahan vektor* $u \oplus v$ *cukup dituliskan dengan u+v, dan operasi perkalian skalar* $k \odot u$ *cukup dituliskan dengan ku.*

Diberikan *F* adalah suatu lapangan dan $n \in \mathbb{N}$, dibentuk himpunan vektor baris dengan panjang *n* atas lapangan *F* yaitu $V_n(F) = \{(x_1, x_2, ..., x_n) : x_1, x_2, ..., x_n \in F\}$. Dapat ditunjukkan bahwa $V_n(F)$ adalah ruang vektor atas *F* terhadap operasi penjumlahan vektor dan perkalian skalar biasa sebagai berikut:

$$(x_1, x_2, ..., x_n) + (y_1, y_2, ..., y_n) = (x_1 + y_1, x_2 + y_2, ..., x_n + y_n)$$

dan

$$k(x_1, x_2, ..., x_n) = (kx_1, kx_2, ..., kx_n)$$

untuk setiap $(x_1, x_2, ..., x_n), (y_1, y_2, ..., y_n) \in V_n(F)$ dan $k \in F$. Dalam penelitian ini, ruang vektor yang digunakan adalah ruang vektor $V_n(F)$ dengan lapangan yang digunakan adalah lapangan hingga $\mathbb{Z}_p$ dengan *p* adalah bilangan prima, sehingga ruang vektor yang digunakan adalah $V_n(\mathbb{Z}_p)$. Dalam kasus khusus, lapangan hingga yang digunakan adalah lapangan biner $\mathbb{Z}_2$, sehingga ruang vektor yang digunakan dalam contoh kasusnya adalah ruang vektor biner $V_n(\mathbb{Z}_2)$.

Definisi 2.2.6. (Anton, 2014) *Diberikan V adalah ruang vektor atas lapangan F. Suatu subset tak kosong* $S \subseteq V$ *disebut dengan* ***subruang*** *dari V jika S merupakan ruang vektor atas F terhadap operasi-operasi yang sama pada V.*

Konsep subruang memainkan peran yang sangat penting dalam penelitian ini. Teknik pengkodean huruf hijaiyah untuk deteksi dan koreksi kesalahan nantinya akan diberikan melalui konsep kode linear yang didefinisikan sebagai subruang dari ruang

vektor $V_n(\mathbb{Z}_p)$, atau dalam kasus lapangan biner adalah sebagai subruang dari ruang vektor biner $V_n(\mathbb{Z}_2)$. Teorema berikut dapat digunakan untuk membantu menentukan apakah suatu himpunan bagian dari sebuah ruang vektor adalah subruang atau bukan.

Contoh 2.2.5. Diberikan ruang vektor biner $V_4(\mathbb{Z}_2)$, maka himpunan bagian dari $V_4(\mathbb{Z}_2)$ yaitu $C=\{(0000),(1010),(0101),(1111)\}$ adalah subruang dari $V_4(\mathbb{Z}_2)$.

Teorema 2.2.2. (Anton, 2014) *Diberikan V adalah ruang vektor atas lapangan F. Suatu subset tak kosong* $S \subseteq V$ *adalah subruang dari V jika dan hanya jika untuk setiap* $u,v \in S$ *dan* $k \in F$ *memenuhi* $u+v \in S$ *dan* $ku \in S$.

Definisi 2.2.7. (Leon, 2002) *Diberikan V adalah ruang vektor atas lapangan F dan himpunan bagian* $B=\{v_1,v_2,...,v_n\} \subseteq V$.

(1) *Himpunan B disebut* ***merentang*** *V jika untuk setiap* $u \in V$ *dapat dinyatakan sebagai* ***kombinasi linear*** *dari vektor-vektor di B, yaitu terdapat* $k_1,k_2,...,k_n \in F$ *sedemikian hingga* $u=k_1v_1+k_2v_2+\cdots+k_nv_n$.

(2) *Himpunan B disebut* ***bebas linear*** *jika* $\bar{0}=k_1v_1+k_2v_2+\cdots+k_nv_n$ *, maka berakibat* $k_1=k_2=\ldots=k_n=0$.

(3) *Himpunan B disebut* ***basis*** *untuk V jika B merentang V dan bebas linear.*

(4) ***Dimensi*** *dari ruang vektor V didefinisikan sebagai banyaknya vektor pada suatu basis untuk ruang vektor V, dinotasikan dengan* $\dim(V)$.

Contoh 2.2.6. Diberikan ruang vektor biner $V_4(\mathbb{Z}_2)$. Diketahui himpunan bagian dari $V_4(\mathbb{Z}_2)$ yaitu $C=\{(0000),(1010),(0101),(1111)\}$ adalah subruang dari $V_4(\mathbb{Z}_2)$. Dapat dilihat bahwa himpunan $B=\{(1000),(0100),(0010),(0001)\}$ adalah basis untuk ruang vektor biner $V_4(\mathbb{Z}_2)$, sehingga dimensi dari $V_4(\mathbb{Z}_2)$ adalah 4. Dapat dilihat juga bahwa subruang *C* memiliki basis $\{(1010),(0101)\}$ sehingga *C* memiliki dimensi 2.

2.2.4. KODE LINEAR

Definisi 2.2.8. (Jurgen Bierbrauer, 2016) *Diberikan F adalah suatu lapangan dan* $n \in \mathbb{N}$*, dibentuk* $V_n(F)$ *ruang vektor atas F. Suatu* ***(n,k)-kode linear*** *C atas F adalah subruang dari* $V_n(F)$ *yang berdimensi k.*

Contoh 2.2.7. Diberikan $C = \{(0000),(1010),(0101),(1111)\}$ adalah subruang dari ruang vektor biner $V_4(\mathbb{Z}_2)$. Diketahui bahwa dimensi dari $V_4(\mathbb{Z}_2)$ adalah 4 dan dimensi dari C adalah 2, maka *C* adalah suatu (4,2)-kode linear atas lapangan biner $\mathbb{Z}_2$.

Berdasarkan hasil penelitian San Ling dan Caophing Xing (2004), proses pembentukan suatu *(n,k)*-kode linear *C* atas lapangan *F* dapat ditentukan melalui pemilihan basis untuk *C* yang disusun dalam sebuah matriks *G*, matriks tersebut dinamakan dengan matriks generator. Diberikan $B = \{v_1, v_2, ..., v_k\} \subseteq V_n(F)$ adalah basis untuk subruang *C* berdimensi *k*, misalkan $v_1 = (a_{11}a_{12}\cdots a_{1n})$, $v_2 = (a_{21}a_{22}\cdots a_{2n})$, ... , $v_k = (a_{k1}a_{k2}\cdots a_{kn})$. Selanjutnya dapat dibentuk matriks generator dari *C* yaitu

$$G = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} \end{pmatrix}.$$

Untuk melakukan pengkodean pada teks pesan yang telah dirubah sebagai elemen dari ruang vektor $V_k \in F$ yaitu $M = (m_1, m_2, ..., m_k) \in V_k(F)$, proses pengkodeannya dilakukan dengan menghitung perkalian matriks

$$MG = (m_1, m_2, ..., m_k) \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} \end{pmatrix},$$
$$= (x_1, x_2, ..., x_n)$$

dan vektor $c=(x_1,x_2,...,x_n)$ disebut dengan katakode (*codeword*) dari *M* setelah dikodekan menggunakan kode linear dengan matriks *G* sebagai matriks generatornya (Vanstone dan Oorschot, 1989). Matriks generator disebut dalam bentuk standar apabila $G=[I_k A]$ dengan I_k adalah matriks identitas berorde *k* dan *A* adalah suatu matriks berukuran $k\times(n-k)$.

Contoh 2.2.8. Diberikan $C=\{(0000),(1010),(0101),(1111)\}$ adalah suatu (4,2)-kode linear atas lapangan biner $\mathbb{Z}_2$. Diketahui bahwa C memiliki basis $\{(1010),(0101)\}$, maka dapat dikonstruksi matriks generator dalam bentuk standar yaitu

$$G=\begin{pmatrix}1&0&1&0\\0&1&0&1\end{pmatrix},$$

sehingga kode linear *C* dapat dinyatakan sebagai

$$\begin{aligned}C&=\{MG: M\in V_2(\mathbb{Z}_2)\}\\&=\left\{M\begin{pmatrix}1&0&1&0\\0&1&0&1\end{pmatrix}: M\in V_2(\mathbb{Z}_2)\right\}\\&=\left\{\begin{pmatrix}x_1&x_2\end{pmatrix}\begin{pmatrix}1&0&1&0\\0&1&0&1\end{pmatrix}: x_1,x_2\in\mathbb{Z}_2\right\}\end{aligned}$$

Definisi 2.2.9. (Vanstone dan Oorschot, 1989) *Diberikan F adalah suatu lapangan dan* $x,y\in V_n(F)$. ***Jarak Hamming*** *dari x dan y, dinotasikan dengan* $d(x,y)$ *didefinisikan sebagai banyaknya posisi koordinat yang berbeda dari x dan y.*

Contoh 2.2.9. Diberikan $x=(10110), y=(11011)\in V_5(\mathbb{Z}_2)$, maka jarak Hamming dari x dan y adalah $d(x,y)=3$.

Definisi 2.2.10. (Vanstone dan Oorschot, 1989) *Diberikan C adalah suatu (n,k)-kode linear atas lapangan F.* ***Jarak Hamming dari C*** *dinotasikan dengan d(C), didefinisikan sebagai*

$$d(C)=\min\{d(x,y): x,y\in C, x\neq y\}.$$

Contoh 2.2.10. Diberikan $C=\{(0000),(1010),(0101),(1111)\}$ adalah suatu (4,2)-kode linear atas lapangan biner $\mathbb{Z}_2$, maka jarak Hamming dari *C* adalah $d(C)=2$.

Berkaitan dengan konsep deteksi dan koreksi adanya kesalahan, yang dimaksud dengan error atau kesalahan adalah apabila vektor yang dikirimkan yaitu $x=(x_1x_2\cdots x_n)$ mengalami perubahan menjadi vektor lain. Dengan demikian, kesalahan yang terjadi adalah adanya beberapa x_i yang nilainya berubah. Sebagai contoh, vektor yang dikirimkan adalah $x=(1010)$, setelah dikirimkam melalui jalur komunikasi kemudian diterima sebagai vektor $y=(0111)$. Dapat dilihat bahwa jarak Hamming dari *x* dan *y* adalah $d(x,y)=1$ yang berarti terjadi 1 kesalahan dalam proses pengiriman.

Contoh 2.2.11. Diberikan *C* adalah suatu (6,2)-kode linear atas $\mathbb{Z}_2$ yang didefinisikan melalui sebuah matriks generator

$$G=\begin{pmatrix}1&0&1&0&1&0\\0&1&0&1&0&1\end{pmatrix}.$$

Diperoleh

$$\begin{aligned}C&=\left\{\begin{pmatrix}x_1&x_2\end{pmatrix}\begin{pmatrix}1&0&1&0&1&0\\0&1&0&1&0&1\end{pmatrix}:x_1,x_2\in\mathbb{Z}_2\right\}\\&=\{(000000),(010101),(101010),(111111)\}\end{aligned}$$

Kode ini dikenal dengan kode perulangan, karena pesan semula yang hanya (00), (01), (10) dan (11), dikodekan menggunakan matriks generator tersebut menjadi (000000), (010101), (101010) dan (111111), artinya terjadi penambahan panjang pesan sebanyak 4 bit, sehingga dari pesan semula memiliki panjang 2 bit, setelah dikodekan menjadi 6 bit. Dapat dilihat bahwa *C* memiliki jarak Hamming $d(C)=3$. Diasumsikan dalam proses pengiriman pesan paling banyak ada 1 kesalahan yang dapat terjadi, artinya ada satu posisi yang nilainya berubah, maka pesan tersebut dapat dikoreksi.

Tabel 2.1. Proses pengkodean pada kode perulangan (6,2)-kode linear atas $\mathbb{Z}_2$

i	m_i	$c_i = m_i G$
0	(00)	(000000)
1	(01)	(010101)
2	(10)	(101010)
3	(11)	(111111)

Sebagai contoh, pesan $m_1 = (01)$ dikodekan menjadi katakode $c_1 = (010101)$, kemudian dikirimkan melalui jalur komunikasi. Misalkan terjadi 1 kesalahan saat proses pengiriman menjadi $x = (010001)$. Dapat dilihat bahwa $d(x, c_0) = 2$, $d(x, c_1) = 1$, $d(x, c_2) = 5$ dan $d(x, c_3) = 4$. Dengan demikian, $x = (010001)$ dikoreksi menjadi (010101) yang berkorespondensi dengan pesan (01).

Teorema 2.2.3. (Vanstone dan Oorschot, 1989*) Diberikan C adalah suatu (n,k)-kode linear atas lapangan F. Jika C memiliki jarak Hamming* $d(C) = d$*, maka C memiliki kemampuan untuk mendeteksi* $d-1$ *kesalahan, serta mampu mengkoreksi* $\left\lfloor \frac{d-1}{2} \right\rfloor$ *kesalahan.*

Contoh 2.2.12. Diberikan *C* adalah suatu (6,2)-kode linear atas $\mathbb{Z}_2$ yang didefinisikan melalui sebuah matriks generator

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix},$$

yaitu $C = \{(000000), (010101), (101010), (111111)\}$ yang memiliki jarak Hamming 3, maka *C* memiliki kemapuan deteksi sebanyak 2 kesalahan serta mempu mengkoreksi sebanyak 1 kesalahan.

Definisi 2.2.11. (Vanstone dan Oorschot, 1989) *Diberikan F adalah lapangan.*

(1) *Bobot Hamming dari* $x \in V_n(F)$ *dinotasikan dengan* $w(x)$*, didefinisikan sebagai banyaknya koordinat tak nol dari x.*

(2) *Diberikan C adalah suatu (n,k)-kode linear atas lapangan F. Bobot Hamming dari C dinotasikan dengan* $w(C)$*, didefinisikan sebagai*

$$w(C) = \min\{w(x) : x \in V_n(F), x \neq 0\}.$$

Contoh 2.2.13. Diberikan *C* adalah suatu (6,2)-kode linear atas $\mathbb{Z}_2$ yang didefinisikan melalui sebuah matriks generator

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix},$$

yaitu $C = \{(000000),(010101),(101010),(111111)\}$. Berdasarkan tabel di bawah ini

Tabel 2.2. Bobot Hamming pada kode perulangan (6,2)-kode linear atas $\mathbb{Z}_2$

i	m_i	$c_i = m_i G$	$w(c_i)$
0	(00)	(000000)	0
1	(01)	(010101)	3
2	(10)	(101010)	3
3	(11)	(111111)	6

Dapat dilihat bahwa *C* memiliki bobot Hamming $w(C) = 3$.

Teorema 2.2.4. (Vanstone dan Oorschot, 1989*) Diberikan C adalah suatu (n,k)-kode linear atas lapangan F, maka* $w(C) = d(C)$.

Definisi 2.2.12. (Vanstone dan Oorschot, 1989) *Diberikan F adalah lapangan dan vektor-vektor* $x = (x_1, x_2, ..., x_n), y = (y_1, y_2, ..., y_n) \in V_n(F)$.

(1) ***Hasil kali dalam*** *(Euclid) dari x dan y didefinisikan sebagai* $\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i$.

(2) Vektor x dan y dikatakan tegak lurus (ortogonal) apabila $\langle x, y \rangle = 0$.

Definisi 2.2.13. (Vanstone dan Oorschot, 1989*) Diberikan C adalah suatu (n,k)-kode linear atas lapangan F. Komplemen tegak lurus dari C dinotasikan dengan* $C^{\perp}$ *dan didefinisikan sebagai* $C^{\perp} = \{x \in V_n(F) : \langle x, y \rangle = 0, \forall y \in C\}$.

Teorema 2.2.5. (Vanstone dan Oorschot, 1989*) Diberikan C adalah suatu (n,k)-kode linear atas lapangan F, maka* $C^{\perp}$ *adalah suatu* $(n, n-k)$*-kode linear atas F. Lebih lanjut, jika* $G = [I_k A]$ *adalah matriks generator untuk C, maka* $H = [-A^T I_{n-k}]$ *adalah matriks generator untuk* $C^{\perp}$*. Selanjutnya, matriks H tersebut dinamakan dengan* ***matriks cek paritas*** *untuk C.*

Diberikan *C* adalah *(n,k)*-kode linear atas *F* dengan matriks generator $G = [I_k A]$. Diberikan pesan yang akan dikodekan yaitu $m = (m_1 m_2 ... m_k) \in V_k(F)$. Menggunakan matriks generator *G* diperoleh pesan yang telah dikodekan berupa katakode $c = mG = m = (m_1 m_2 ... m_k x_1 x_2 ... x_{n-k}) \in V_n(F)$. Penambahan vektor $(x_1 x_2 ... x_{n-k})$ pada *m* disebut dengan cek simbol. Pada kasus lapangan biner, maka penambahan vektor tersebut dinamakan dengan cek bit. Dikarenakan *G* adalah matriks generator untuk C, dan H adalah matriks generator untuk $C^{\perp}$, maka untuk setiap $x \in C$ pasti memenuhi $Hx^T = 0$, dengan 0 yang dimaksud adalah vektor nol dalam bentuk kolom. Dengan demikian, dapat disimpulkan bahwa kata kode *c* tidak terdeteksi error jika dan hanya jika $Hc^T = 0$, dan terdeteksi error jika dan hanya jika $Hc^T \neq 0$.

Contoh 2.2.14. Diberikan *C* adalah suatu (6,2)-kode linear atas $\mathbb{Z}_2$ yang didefinisikan melalui sebuah matriks generator

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix},$$

yaitu $C = \{(000000), (010101), (101010), (111111)\}$. Berdasarkan matiks generator *G* tersebut, dapat diperoleh matriks cek paritas

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Misalkan diterima vektor $x = (010001)$, dengan menghitung Hx^T diperoleh

$$Hx^T = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Dapat dilihat bahwa $Hx^T \neq 0$, sehingga $x \notin C$, yaitu terdeteksi adanya kesalahan.

Teorema 2.2.6. (Vanstone dan Oorschot, 1989*) Diberikan H adalah matriks cek paritas untuk (n,k)-kode linear C atas F, maka setiap himpunan yang terdiri dari sebanyak s-1 kolom dari H adalah himpunan bebas linear jika dan hanya jika C memiliki jarak Hamming paling sedikit adalah s.*

Teorema di atas dapat digunakan untuk mengkonstruksi sebuah kode yang dapat mengkoreksi 1 kesalahan (single error correcting code). Caranya adalah dengan mengkonstruksi matriks cek paritas *H* sedemikian hingga tidak ada sebanyak 2 atau lebih kolom-kolomnya yang tidak bebas linear, yaitu ada kolom yang merupakan kombinasi dari kolom-kolom yang lainnya.

Definisi 2.2.14. (Vanstone dan Oorschot, 1989*) Suatu **kode Hamming** berorder r atas lapangan F dengan* $|F| = q$ *adalah suatu (n,k)-kode linea C atas F dengan* $n = \frac{q^r - 1}{q - 1}$ *dan* $k = n - r$*. Matriks cek paritasnya adalah matriks* H_r *berukuran r x n sedemikian hingga kolom-kolom dari* H_r *tidak nol dan tidak ada dua kolom yang merupakan hasil kali skalar satu sama lain.*

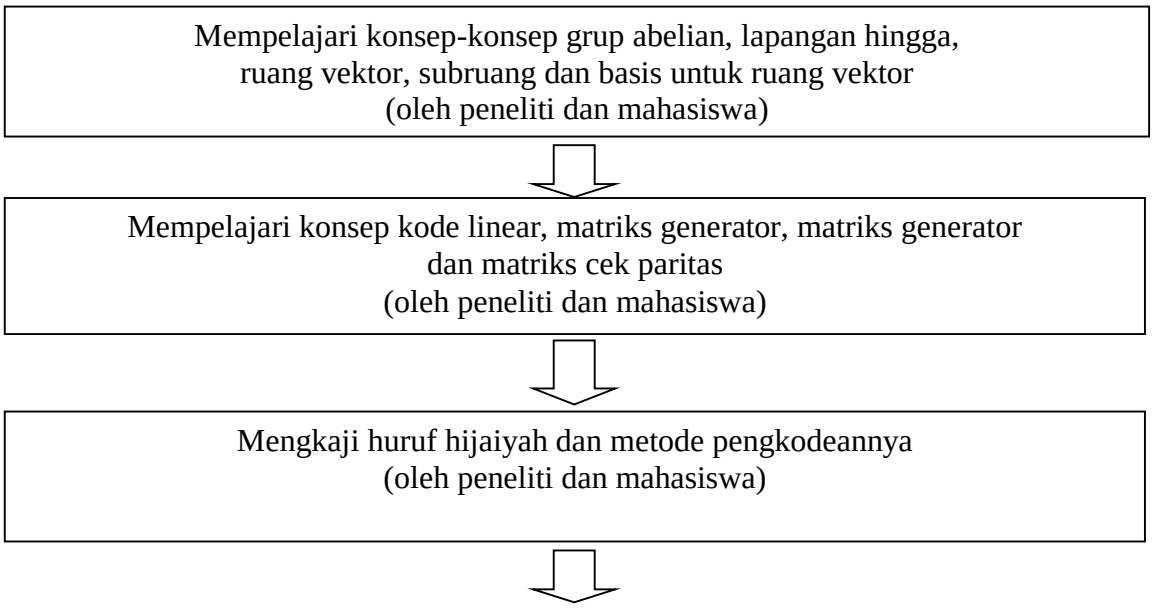
Berdasarkan konstruksi kode Hamming di atas, dapat dilihat dengan jelas bahwa kode Hamming memiliki jarak Hamming 3, sehingga memiliki kemampuan mendeteksi 2 kesalahan, serta mampu mengkoreksi 1 kesalahan. Oleh karena itu, kode Hamming adalah sebuah *single error correcting code*.

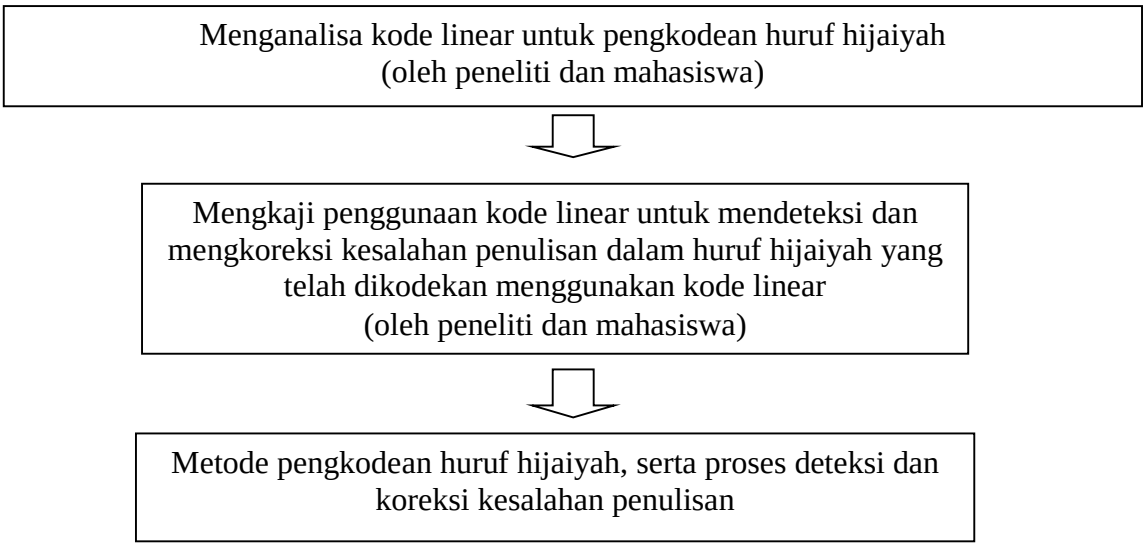
BAB III
METODE PENELITIAN DAN IMPLEMENTASINYA

3.1. METODE PENELITIAN

Dalam penelitian tentang pengkodean huruf hijaiyah ini digunakan metode studi literatur yang tediri dari jurnal-jurnal ilmiah yang berkaitan dengan penelitian, dan buku-buku referensi yang mendukung penelitian. Langkah pertama yang dilakukan peneliti adalah dengan mempelajari konsep-konsep grup abelian, lapangan hingga, ruang vektor, subruang dan basis untuk ruang vektor. Setelah itu dikaji konsep-konsep kode linear, matriks generator, matriks generator dan matriks cek paritas.

Penelitian ini memiliki latar belakang tentang kasus kesalahan penulisan ayat Al-Qur'an, sehingga peneliti melakukan kajian tentang huruf hijaiyah dan metode pengkodeannya melalui sebuah korespondensi satu-satu dengan bilangan atau vektor. Selanjutnya, dilakukan analisa penggunaan kode linear untuk pengkodean huruf hijaiyah agar dapat dideteksi dan dikoreksi apabila terjadi kesalahan tertentu. Langkah selanjutnya, peneliti mengkaji penggunaan kode linear untuk mendeteksi dan mengkoreksi kesalahan penulisan dalam huruf hijaiyah yang telah dikodekan menggunakan kode linear. Alur penelitian secara utuh diberikan dalam bagan alir penelitian berikut ini.





Gambar 3.1. Bagan alir penelitian

3.2. IMPLEMENTASI PENELITIAN

Seringkali hasil penelitian hanya tersimpan di perpustakan dalam bentuk Laporan Penelitian. Namun, target hasil penelitian ini adalah publikasi dalam bentuk karya ilmiah jurnal nasional. Implementasi penelitian ini dijadwalkan sebagai berikut :

No	Tahap	Bulan					
		I	II	III	IV	V	VI
1.	Studi Literatur	■					
2.	Koordinasi Peneliti dan Mahasiswa	■					
3.	Survey Materi Struktur Aljabar, Aljabar Linear dan Pengkodean Huruf Hijaiyah	■					
4.	Konstruksi Kode Linear Melalui Matriks Generator		■				
5.	Pengkodean Huruf Hijaiyah dan Ayat Al-Qur'an			■	■		
6.	Deteksi dan Koreksi Kesalahan				■	■	
7.	Penulisan Draft Artikel Jurnal					■	■
8.	Konsultasi dan Penyusunan Laporan, Pengiriman Artikel Jurnal						■

Penguatan kompetensi peneliti akan berpengaruh pada kualitas hasil penelitian. Oleh karena itu, tim peneliti selalu memanfaatkan kesempatan untuk mengikuti acara-acara ilmiah bidang aljabar, seperti seminar, *short course*, workshop baik tingkat nasional maupun internasional. Berikut diberikan kegiatan-kegiatan tim peneliti untuk menguatkan kompetensi :

1. Ketua peneliti mengikuti kegiatan *short course* bertaraf internasional yaitu the SEAMS-UGM-ITB Summer Course on Coding Theory and Cryptography yang dilaksanakan di Universitas Gadjah Mada Yogyakarta pada tanggal 15-26 Juli 2019. Kegiatan ini diikuti oleh peserta dari negara-negara di Asia Tenggara. Topik utama yang dibahas dalam kegiatan tersebut adalah perkembangan teori pengkodean seperti kode linear, serta perkembangan dalam kriptografi. Selama mengikuti kegiatan tersebut, peneliti mendapatkan banyak sekali ide-ide baru yang berkaitan dengan kriptografi dan teori pengkodean yang bermanfaat dalam penelitian ini.
2. Ketua peneliti mengikuti dan menjadi pemakalah dalam kegiatan Seminar Nasional Integrasi Matematika dan Nilai Islam yang diselenggarakan di Universitas Islam Negeri Maulana Malik Ibrahim di Malang Jawa Timur pada tanggal 21 September 2019. Dalam kegiatan tersebut, peneliti memaparkan studi awal penelitian terkait dengan penerapan ilmu aljabar pada teori pengkodean untuk deteksi dan koreksi kesalahan penulisan dalam huruf hijaiyah. Peneliti juga mendapatkan beberapa kritik dan saran terkait dengan materi presentasi.
3. Ketua peneliti mengikuti kegitan Workshop on Maxima: A Computer Algebra System yang diselenggarakan di FMIPA Universitas Negeri Yogyakarta pada tanggal 2-3 Oktober 2019. Dalam kegiatan tersebut, peneliti mendapatkan pengetahuan dan ketrampilan dalam menggunakan *software* yang dapat digunakan untuk membantu perhitungan aljabar yang kompleks dan rumit apabila dikerjakan secara manual.

3.3. PERSONALIA

Peneliti dibantu oleh dua orang asisten peneliti yang juga merupakan mahasiswa Program Studi Matematika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta. Asisten peneliti yang pertama adalah Saudari Yenni Karitka, mahasiswi angkatan 2016 yang saat ini mengambil topik skripsi tentang penerapan struktur aljabar

dalam teori pengkodean. Asisten peneliti yang kedua adalah Saudari Nenti Ekta Monita Larasati, mahasiswi angkatan 2016 yang saat ini mengambil topik skripsi tentang struktur aljabar. Kedua asisten peneliti tersebut membantu peneliti dalam proses perhitungan pengkodean yang melibatkan operasi perkalian matriks, serta membantu proses perhitungan dalam mendeteksi dan mengkoreksi kesalahan menggunakan matriks cek paritas.

BAB IV
HASIL PENELITIAN DAN PEMBAHASAN

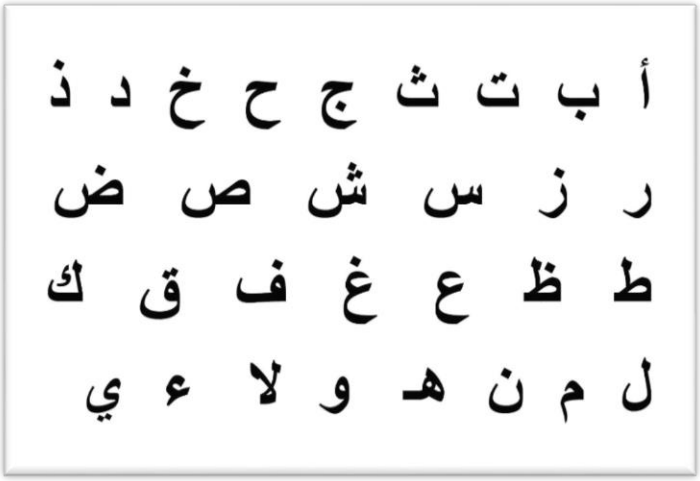
4.1. KOREPSONDENSI HURUF HIJAIYAH

Dalam penelitian ini, teks yang akan dikodekan menggunakan kode linear adalah berupa ayat-ayat Al-Qur'an yang ditulis menggunakan huruf hijaiyah. Untuk merubah ayat-ayat menjadi angka-angka yang merepresentasikan ayat tersebut menjadi vektor pada ruang vektor $V_k(F)$. Penelitian yang berkaitan dengan pengkodean huruf hijaiyah telah dilakukan oleh Yahya Alqahtani dkk (2013) yang kemudian disempurnakan pada penelitian oleh Prakash Kuppuswamy dan Yahya Alqahtani (2014) untuk keperluan enkripsi pesan rahasia dalam huruh hijaiyah, dalam penelitian tersebut digunakan korespondensi seperti pada tabel berikut.

Tabel 4.1. Korespondensi huruf hijaiyah dengan bilangan
(Prakash Kuppuswamy dan Yahya Alqahtani, 2014)

1	2	3	4	5	6	7	8	9	10	11	12	13
أ	ب	ت	ث	ج	ح	خ	د	ذ	ر	ز	س ص	ش
14	15	16	17	18	19	20	21	22	23	24	25	26
ط	ظ ض	ع	غ	ف	ق	ك	ل	م	ن	هـ	و	ي
27	28	29	30	31	32	33	34	35	36	37		
٠	١	٢	٣	٤	٥	٦	٧	٨	٩	blank		

Perkembangan pengkodean huruf hijaiyah kemudian dilakukan oleh Ameer Kadhim Hadi (2017) dalam penelitiannya untuk pengamanan pesan singkat SMS. Dikarenakan dalam al-Qur'an tidak memuat angka dalam ayatnya, maka peneliti tidak memasukkan angka sebagai bagian dari huruf hijaiyah yang digunakan, sehingga diperoleh sebanyak 30 huruf hijaiyah, seperti diberikan dalam gambar di bawah ini.



Gambar 4.1. Huruf hijaiyah (30 huruf)

Metode korespondensi yang sederhana dan melibatkan struktur aljabar yang telah dijelaskan dalam konsep grup dan ring, maka dapat digunakan himpunan semua bilangan bulat modulo $\mathbb{Z}_{30} = \{0,1,2,...,29\}$ dengan korespondensinya adalah huruf "alif" dikorespondensikan dengan 0, huruf "ba" dikorespondensikan dengan 1, begitu seterusnya sampai dengan huruf "ya" yang dikorespondensikan dengan 29.

Himpunan $\mathbb{Z}_{30}$ memiliki struktur aljabar berupa ring komutatif dengan elemen satuan, tetapi bukan lapangan, sebab 30 bukan bilangan prima. Oleh karena itu, tidak dapat digunakan untuk mengkonstruksi kode linear yang syarat utamanya adalah penggunaan struktur aljabar berupa lapangan. Oleh karena itu, peneliti mengusulkan penggunakan himpunan $\mathbb{Z}_{31} = \{0,1,2,...,30\}$ dengan 31 adalah bilangan prima, hal ini dilakukan untuk mengakomodir syarat sebagai lapangan. Korespondensi yang terbentuk adalah huruf "alif" dikorespondensikan dengan 1, huruf "ba" dikorespondensikan dengan 2, begitu seterusnya sampai dengan huruf "ya" yang dikorespondensikan dengan 30.

Misalkan digunakan lapangan hingga $\mathbb{Z}_{31} = \{0,1,2,...,30\}$. Apabila digunakan kode Hamming dengan order 2 saja, maka diperoleh n=32 dan k=30, diperoleh matriks generator yang cukup besar, memiliki ukuran 30x32 dengan entri dari himpunan $\mathbb{Z}_{31}$. Apabila digunakan kode Hamming dengan order 3, maka diperoleh n=993 dan k=990, sebuah matriks generator yang sangat besar karena memiliki ukuran 990x993. Oleh

karena itu, diperlukan teknik korespondensi yang dapat menghasilkan matriks yang lebih kecil sehingga proses perhitungan pengkodean dapat berjalan lebih efisien.

Teknik korespondensi satu-satu yang digunakan untuk mengatasi masalah matriks generator yang besar adalah dengan melakukan ekspansi biner dari semua bilangan yang termuat dalam lapangan $\mathbb{Z}_{31}$, yaitu dengan cara menuliskan masing-masing bilangan sebagai vektor biner basis 2. Sebagai contohnya, bilangan 10 dapat dituliskan sebagai 10 = 8 + 2 atau 10 = 1.8 + 0.4 + 1.2 + 0.1, sehingga bilangan 10 berkorespondensi dengan vektor biner (1010). Bilangan terbesar yang mungkin adalah 30, diperoleh 30 = 1.16 + 1.8 + 1.4 + 1.2 + 0.1, sehingga 30 berkorespondensi dengan vektor biner (11110) yang memiliki panjang 5. Dengan demikian, masing-masing huruf hijaiyah dikodekan menjadi vektor biner dengan panjang 5 atau lebih dikenal dengan 5-bit, seperti diberikan dalam tabel di bawah ini.

Tabel 4.2. Korespondensi huruf hijaiyah dan vektor biner

أ	1	00001	ح	6	000110
ب	2	00010	خ	7	000111
ت	3	00011	د	8	01000
ث	4	00100	ذ	9	01001
ج	5	00101	ر	10	01010
ز	11	01011	ط	16	10000
س	12	01100	ظ	17	10001
ش	13	01101	ع	18	10010
ص	14	01110	غ	19	10011
ض	15	01111	ف	20	10100

ق	21	10101	ه	26	11010
ك	22	10110	و	27	11011
ل	23	10111	لا	28	11100
م	24	11000	ء	29	11101
ن	25	11001	ي	30	11110

4.2. KODE LINEAR ATAS LAPANGAN BINER UNTUK HURUF HIJAIYAH

Berdasarkan korespondensi yang telah diberikan pada Tabel 4.2. di atas, maka kode linear yang digunakan didefinisikan atas lapangan biner $\mathbb{Z}_2$. Setiap huruf hijaiyah dinyatakan sebagai vektor biner 5 bit, sehingga himpunan semua pesan awal yang belum dikodekan adalah $V_5(\mathbb{Z}_2) = \{(x_1x_2x_3x_4x_5) : x_1, x_2, x_3, x_4, x_5 \in \mathbb{Z}_2\}$.

Apabila diasumsikan terjadi satu kesalahan, yaitu satu huruf berubah menjadi huruf yang lain, maka artinya terdapat terjadi paling banyak 5 kesalahan. Apabila digunakan kode Hamming atas lapangan biner, maka harus dikonstruksi kode linear dengan jarak Hammingnya adalah 11. Oleh karena itu, matriks generator yang dikonstruksi masih sangat besar.

Untuk dapat menyiasati penggunaan kode Hamming yang memiliki kemampuan koreksi hanya 1 kesalahan saja, untuk dapat digunakan dalam mengkoreksi kelasahan 1 huruf hijaiyah, diasumsikan bahwa dapat terjadi perubahan satu huruf menjadi huruf lain dalam setiap blok yang terdiri dari 4 huruf. Misalkan dalam setiap blok terdiri dari 4 huruf, yaitu:

Huruf ke-1: $(a_1b_1c_1d_1e_1) \in V_5(\mathbb{Z}_2)$

Huruf ke-2: $(a_2b_2c_2d_2e_2) \in V_5(\mathbb{Z}_2)$

Huruf ke-3: $(a_3b_3c_3d_3e_3) \in V_5(\mathbb{Z}_2)$

Huruf ke-4: $(a_4b_4c_4d_4e_4) \in V_5(\mathbb{Z}_2)$

Selanjutnya, dibentuk vektor-vektor sebagai berikut:

$$a=(a_1a_2a_3a_4)\in V_4(\mathbb{Z}_2)$$

$$b=(b_1b_2b_3b_4)\in V_4(\mathbb{Z}_2)$$

$$c=(c_1c_2c_3c_4)\in V_4(\mathbb{Z}_2)$$

$$d=(d_1d_2d_3d_4)\in V_4(\mathbb{Z}_2)$$

$$e=(e_1e_2e_3e_4)\in V_4(\mathbb{Z}_2)$$

Dengan cara seperti ini, apabila terjadi satu kesalahan berupa berubahnya satu huruf menjadi huruf lain dalam setiap blok, maka artinya terjadi kesalahan dalam 1 bit pada setiap vektor *a, b, c, d* dan *e*. Oleh karena itu, dapat digunakan kode Hamming dengan order 3 atas lapangan biner $\mathbb{Z}_2$. Berdasarkan parameter yang disyaratkan dalam kode Hamming, dengan $q=|\mathbb{Z}_2|=2$, maka diperoleh $n=\frac{2^3-1}{2-1}=7$ dan $k=7-3=4$. Akan dikonstruksi sebuah (7,4)-kode linear atas $\mathbb{Z}_2$ dengan jarak Hamming 3.

Sebagai contohnya, dikonstruksi matriks cek paritas yang memenuhi ketentuan yang disyaratkan dalam kode Hamming, yaitu tidak memuat kolom nol, dan tidak ada sebuah kolom yang merupakan hasil kali skalar dari kolom yang lain, yaitu

$$H=\begin{pmatrix}1&0&1&1&1&0&0\\1&1&0&1&0&1&0\\0&1&1&1&0&0&1\end{pmatrix}.$$

Apabila dinyatakan dalam bentuk standar, diperoleh $H=\left[-A^T I_3\right]$ dengan

$$-A^T=\begin{pmatrix}1&0&1&1\\1&1&0&1\\0&1&1&1\end{pmatrix},$$

sehingga diperoleh

$$A=\begin{pmatrix}1&1&0\\0&1&1\\1&0&1\\1&1&1\end{pmatrix}.$$

Selanjutnya, ditentukan matriks generator dari *C* yaitu

$$G = [I_4 A] = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Diperoleh himpunan $C = \{a' = aG, b' = bG, c' = cG, d' = dG, e' = eG\}$ dan tabel berikut:

M	MG
$a = (a_1 a_2 a_3 a_4)$	$a' = (a_1 a_2 a_3 a_4 a_5 a_6 a_7)$
$b = (b_1 b_2 b_3 b_4)$	$b' = (b_1 b_2 b_3 b_4 b_5 b_6 b_7)$
$c = (c_1 c_2 c_3 c_4)$	$c' = (c_1 c_2 c_3 c_4 c_5 c_6 c_7)$
$d = (d_1 d_2 d_3 d_4)$	$d' = (d_1 d_2 d_3 d_4 d_5 d_6 d_7)$
$e = (e_1 e_2 e_3 e_4)$	$e' = (e_1 e_2 e_3 e_4 e_5 e_6 e_7)$

Setelah itu, kata kode yang diperoleh disusun kembali, sehingga diperoleh 4 huruf pertama dan 15 bit tambahannya, yaitu:

Huruf ke-1: $(a_1 b_1 c_1 d_1 e_1)$ Huruf ke-2: $(a_2 b_2 c_2 d_2 e_2)$

Huruf ke-3: $(a_3 b_3 c_3 d_3 e_3)$ Huruf ke-4: $(a_4 b_4 c_4 d_4 e_4)$,

Cek bit ke-1 : $(a_5 b_5 c_5 d_5 e_5)$, Cek bit ke-2: $(a_6 b_6 c_6 d_6 e_6)$,

Cek bit ke-3: $(a_7 b_7 c_7 d_7 e_7)$

Masing-masing vektor di *C* memiliki panjang 7-bit, yaitu terjadi penambahan sebanyak 3 bit. Oleh karena itu, total penambahan bit dalam setiap blok adalah 15 bit, hal ini berarti dari 1 blok pesan yang memiliki panjang 20 bit menjadi 35 bit. Penambahan 15 bit tersebut dinamakan dengan cek bit.

Contoh 4.1. Misalkan akan dikodekan pesan dalam huruf hijaiyah sebagai berikut:

م ت س ي

Berdasarkan Tabel 4.2. di atas, diperoleh korespondensi antara huruf hijaiyah dan vektor biner sebegai berikut:

م	11000
ت	00011
س	01100
ي	11110

Berdasarkan konstruksi kode linearnya, diperoleh $a=(1001)$, $b=(1011)$, $c=(0011)$, $d=(0101)$ dan $e=(0100)$. Selanjutnya, dilakukan pengkodean dengan mengalikannya dengan matriks generator, diperoleh:

$$a'=aG=(1001)\begin{pmatrix}1&0&0&0&1&1&0\\0&1&0&0&0&1&1\\0&0&1&0&1&0&1\\0&0&0&1&1&1&1\end{pmatrix}=(1001001)$$

$$b'=bG=(1011)\begin{pmatrix}1&0&0&0&1&1&0\\0&1&0&0&0&1&1\\0&0&1&0&1&0&1\\0&0&0&1&1&1&1\end{pmatrix}=(1011100)$$

$$c'=cG=(0011)\begin{pmatrix}1&0&0&0&1&1&0\\0&1&0&0&0&1&1\\0&0&1&0&1&0&1\\0&0&0&1&1&1&1\end{pmatrix}=(0011010)$$

$$d'=dG=(0101)\begin{pmatrix}1&0&0&0&1&1&0\\0&1&0&0&0&1&1\\0&0&1&0&1&0&1\\0&0&0&1&1&1&1\end{pmatrix}=(0101100)$$

$$e' = eG = (0100)\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} = (0100011)$$

Diperoleh hasil pengkodean sebagai berikut:

M	MG
$a = (1001)$	$a' = (1001001)$
$b = (1011)$	$b' = (1011100)$
$c = (0011)$	$c' = (0011010)$
$d = (0101)$	$d' = (0101100)$
$e = (0100)$	$e' = (0100011)$

Pesan yang telah dikodekan adalah sebagai berikut:

م ت س ي

Cek bit: 01010 00101 10001

Apabila cek bit dapat ditulis dalam huruf hijaiyah sesuai dengan tabel, diperoleh pesan yang telah dikodekan sebagai berikut:

م ت س ي ر ج ظ

4.3. DETEKSI DAN KOREKSI KESALAHAN

Diberikan C adalah *(n,k)*-kode linear atas lapangan F. Misalkan H adalah matriks cek paritas untuk C. Diberikan katakode $c \in C$, apabila terjadi satu kesalahan maka ada satu koordinat yang nilainya berubah, misalkan $E \in V_n(F)$ adalah vektor kesalahan sedemikian hingga pesan yang telah mengalami 1 kesalahan adalah $x = c + E$.

Apabila terjadi 1 kesalahan, maka *E* adalah vektor yang entrinya adalah 0 kecuali untuk satu koordinat, serta diketahui $Hx^T \neq 0$, diperoleh

$$Hx^T = H\left(c+E\right)^T = H\left(c^T + E^T\right) = Hc^T + HE^T = 0 + HE^T = HE^T .$$

Oleh karena itu, HE^T muncul sebagai hasil kali skalar dari suatu kolom dalam H yang menunjukkan lokasi kesalahannya. Apabila digunakan lapangan biner, maka koordinat terjadinya kesalahan dapat dilihat dari kolom dari *H* dimana vektor kolom HE^T muncul.

Untuk mendeteksi adanya kesalahan, misalkan diterima vektor-vektor berikut ini:

Huruf ke-1: $\left(a_1b_1c_1d_1e_1\right)$ Huruf ke-2: $\left(a_2b_2c_2d_2e_2\right)$ Huruf ke-3: $\left(a_3b_3c_3d_3e_3\right)$

Huruf ke-4: $\left(a_4b_4c_4d_4e_4\right)$, Cek bit ke-1 : $\left(a_5b_5c_5d_5e_5\right)$, Cek bit ke-2: $\left(a_6b_6c_6d_6e_6\right)$,

Cek bit ke-3: $\left(a_7b_7c_7d_7e_7\right)$

Langkah selanjutnya, disusun vektor-vektor $a' = \left(a_1a_2a_3a_4a_5a_6a_7\right)$, $b' = \left(b_1b_2b_3b_4b_5b_6b_7\right)$ $c' = \left(c_1c_2c_3c_4c_5c_6c_7\right)$, $d' = \left(d_1d_2d_3d_4d_5d_6d_7\right)$ dan $e' = \left(e_1e_2e_3e_4e_5e_6e_7\right)$. Untuk mendeteksi adanya kesalahan, digunakan matriks cek paritas *H*, yaitu dengan menghitung $H\left(a'\right)^T$, $H\left(b'\right)^T$, $H\left(\mathrm{c}'\right)^T$, $H\left(d'\right)^T$ dan $H\left(e'\right)^T$. Apabila diperoleh hasil vektor yang tidak nol, maka terdeteksi adanya kesalahan.

Untuk proses koreksi yang diakibatkan oleh 1 kesalahan, langkah-langkahnya adalah dengan melihat hasil perhitungan $H\left(a'\right)^T$, $H\left(b'\right)^T$, $H\left(\mathrm{c}'\right)^T$, $H\left(d'\right)^T$ dan $H\left(e'\right)^T$. Apabila ditemukan hasil berupa vektor tak nol, maka hasil vektor tersebut dilihat di dalam matriks cek paritas *H*. Posisi koordinat terjadinya kesalahan terletak di posisi kolom dimana vektor tersebut muncul. Cara mengkoreksinya hanya dengan mengganti 0 dengan 1 atau sebaliknya.

Contoh 4.2. Diberikan kode Hamming dengan parameter dan kasus seperti pada Contoh 4.1. di atas, misalkan diterima pesan yang telah terjadi 1 kesalahan yaitu:

م ن س ي ر ج ظ

Langkah pertama adalah merubah setiap huruf menjadi vektor biner sesuai dengan tabel korespondensi, yaitu

م	11000
ن	11001
س	01100
ي	11110
ر	01010
ج	00101
ظ	10001

Selanjutnya, dibentuk vektor-vektor $a'=(1101001)$, $b'=(1111100)$, $c'=(0011010)$, $d'=(0001100)$ dan $e'=(0100010)$. Untuk melakukan deteksi kesalahan dilakukan proses perhitungan berikut:

$$H(a')^T=\begin{pmatrix}1&0&1&1&1&0&0\\1&1&0&1&0&1&0\\0&1&1&1&0&0&1\end{pmatrix}(1101001)^T=\begin{pmatrix}0\\1\\1\end{pmatrix}\neq\begin{pmatrix}0\\0\\0\end{pmatrix}$$

$$H(b')^T=\begin{pmatrix}1&0&1&1&1&0&0\\1&1&0&1&0&1&0\\0&1&1&1&0&0&1\end{pmatrix}(1111100)^T=\begin{pmatrix}0\\1\\1\end{pmatrix}\neq\begin{pmatrix}0\\0\\0\end{pmatrix}$$

$$H(c')^T=\begin{pmatrix}1&0&1&1&1&0&0\\1&1&0&1&0&1&0\\0&1&1&1&0&0&1\end{pmatrix}(0011010)^T=\begin{pmatrix}0\\0\\0\end{pmatrix}$$

$$H(d')^T = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} (0001100)^T = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$H(e')^T = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} (0100010)^T = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Berdasarkan hasil perhitungan di atas, diperoleh bahwa terjadi kesalahan pada vektor a', b' dan d'. Dapat dilihat bahwa $H(a')^T = H(b')^T = H(d')^T = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$ muncul sebagai kolom kedua dari matriks cek paritas *H*. Oleh karena itu, kesalahan terjadi pada bit ke-2, sehingga vektor kesalahannya adalah $E = (0100000)$. Proses koreksi dilakukan dengan menghitung:

$$a' - E = (1101001) - (0100000) = (1001001)$$
$$b' - E = (1111100) - (0100000) = (1011100)$$
$$d' - E = (0001100) - (0100000) = (0101100)$$

Diperoleh katakode - katakode yang telah dikoreksi, yaitu (1001001), (1011100), (0011010), (0101100) dan (0100011). Selanjutnya, cek bit dihilangkan, diperoleh (1001), (1011), (0011), (0101) dan (0100). Kemudian disusun dalam tabel berikut:

11000	م
00011	ت
01100	س
11110	ي

Diperoleh pesan semula yaitu

م ت س ي

Berdasarkan perhitungan-perhitungan di atas, maka dapat disimpulkan bahwa kode Hamming berorder 3 atas lapangan $\mathbb{Z}_2$ dapat digunakan untuk mendeteksi dan mengkoreksi kesalahan penulisan dalam huruf hijaiyah untuk jenis kesalahan tertentu, yaitu dalam setiap blok pesan yang terdiri dari 4 huruf, terjadi perubahan sebuah huruf menjadi huruf yang lainnya. Hal tersebut terjadi dikarenakan kode Hamming hanya memiliki kemampuan koreksi 1 kesalahan. Apabila diinginkan dapat mengkoreksi 2 kesalahan, maka harus digunakan kode linear dengan jarak Hammingnya adalah 5, yang mengakibatkan matriks generatornya menjadi lebih besar, serta penambahan cek bit yang lebih banyak.

BAB V
PENUTUP

5.1. KESIMPULAN

Dalam penelitian ini, dihasilkan beberapa kesimpulan sebagai berikut:

1. Cara mengkonstruksi korespondensi huruf hijaiyah dilakukan melalui ekspansi biner pada urutan huruf-huruf hijaiyah yang berjumlah 30 huruf, dimulai dari huruf “alif” yang dikorespondensikan dengan bilangan 1 yang memiliki ekspansi biner 5 bit yaitu 00001, sampai dengan huruf ‘ya” yang dikorespondensikan dengan bilangan 30 yang memiliki ekspansi biner 5 bit yaitu 11110. Dari 4 huruf tersebut kemudian disusun dalam matriks, kemudian dibentuk 5 vektor dengan panjang 4 bit yang diambil pada kolom-kolomnya. Pengkodean yang digunakan berupa kode linear berupa kode Hamming atas lapangan biner $\mathbb{Z}_2$ dengan matriks generatornya adalah

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

   Terjadi penambahan panjang pesan sebanyak 15 bit, dari yang semula 20 bit, setelah dikodekan menjadi 35 bit.

2. Berdasarkan penggunaan kode Hamming atas lapangan biner $\mathbb{Z}_2$ dengan order 3, maka jenis kesalahan yang dapat dideteksi dan dikoreksi adalah apabila terjadi kesalahan penulisan dalam setiap blok yang terdiri dari 4 huruf, terjadi kejadian satu huruf menjadi huruf yang lain.
3. Untuk menndeteksi dan mengkoreksi adanya kesalahan penulisan dalam huruf hijaiyah yang telah dikodekan menggunakan kode linear berupa kode Hamming atas lapangan biner $\mathbb{Z}_2$ berorder 3, digunakan matriks cek paritas:

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

5.2. SARAN

1. Perlu dikaji jenis-jenis kode lain yang lebih cocok digunakan untuk pengkodean huruf hijaiyah, sehingga dapat meminimalisir jumlah penambahan cek bit pada pesan semula.
2. Perlu dikaji jenis-jenis kesalahan penulisan apa saja yang sering muncul pada penulisan dalam huruf hijaiyah.
3. Perlu dikaji metode pengkodean untuk jenis kesalahan yang terjadi karena adanya penambahan huruf baru dalam sebuah pesan, serta jenis kesalahan yang terjadi karena adanya penghapusan huruf.

DAFTAR PUSTAKA

Ameer Kadhim Hadi. 2017. *Toward Trust and More Characters of Arabic Short Message Service using Encryption*. Journal of Engineering and Applied Sciences. Vol.12 No.21. pp.5384-5387.

Anton, Howard. 2014. *Elementary Linear Algebra* 11*th Edition: Applications Version*. Canada. Wiley.

Dummit, David S. dan Foote Richard M. 2004. *Abstract Algebra Third Edition*. New Jersey: John Wiley and Sons.

Jurgen Bierbrauer. 2016. *Introduction to Coding Theory* 2*nd Edition*. Boca Raton Florida. Chapman and Hall/CRC.

Leon, Steven J. 2002. *Linear Algebra with Applications* 6*th Edition*. New Jersey. Prentice-Hall.

Malik, D.S., Morderson John N. dan Sen, M.K. 1997. *Fundamentals of Abstract Algebra*. WCB/McGraw-Hill.

Prakash Kuppuswamy dan Yahya Alqahtani. 2014. *New Innovation of Arabic Language Encryption Technique Using New Symmetric Key Algorithm*. International Journal of Advances in Engineering & Technology. Vol. 7 Issue 1. Mar 2014. pp. 30-37.

Republika. 2017. *Kesalahan Penulisan Alquran, Penyeleksian Harus Diperluas*. https://www.republika.co.id/berita/dunia-islam/islam-nusantara/17/10/29/oyl5es396-kesalahan-penulisan-alquran-penyeleksian-harus-diperluas (diakses tanggal 1 September 2018)

San Ling, Chaoping Xing. 2004. *Coding Theory: A First Course*. Cambridge UK. Cambridge University Press.

Shannon, Claude. 1948. *A Mathematical Theory of Communication*. Bell System Technical Journal. 27 (3). Pp.379-423.

Thomas W. Judson. 2017. *Abstract Algebra : Theory and Applications:* 2017 *Edition*. Texas. Orthogonal Publishing L3C.

Van Lint, J.H. 1999. *Introduction to Coding Theory Third Edition*. Springer.

Vanstone, Scott A. dan Oorschot, Paul C. van. 1989. *An Introduction to Error Correcting Codes with Applications*. Kluwer Academic Publishers.

William E. Ryan dan Shu Lin. 2009. *Channel Codes: Classical and Modern*. Cambridge University Press.

Yahya Alqahtani, Prakash Kuppuswamy dan Sikandhar Shah. 2013. *New Approach of Arabic Encryption/Decryption Technique Using Vigenere Cipher on Mod* 39. International Journal of Advanced Research in IT and Engineering. Vol.2 No.12. Dec 2013. pp.1-9.